Referência : Processo nº 202303000392278

Assunto : Resposta aos questionamentos.

QUESTIONAMENTOS E RESPOSTAS – EDITAL Nº 67/2023

Data do e-mail: 28/8/2023.

1) Em relação à distribuição dos agentes ou sensores a serem instalados no ambiente do TJGO, compreendemos que o Tribunal de Justiça do Estado de Goiás (TJGO) dispõe de uma plataforma de distribuição dedicada, que viabiliza a implantação em larga escala no referido ambiente. Isso se torna particularmente relevante, dado o considerável número de 20.000 endpoints a serem contemplados. Está correto o entendimento?

Resposta: Está correto o entendimento. O TJGO dispõe da funcionalidade de instalação dos agentes/sensores via Microsoft GPO e no caso de sistemas Linux, a opção de utilização do Puppet.
Ressaltamos que, a Seção 17 do Termo de Referência prevê a possibilidade de agendamento de vistoria técnica, caso as empresas interessadas tenham dúvidas técnicas.

2) Referente ao item "*1.21 A solução deve possibilitar a definição de lista de IPs especificas limitando o acesso a console de administração para uma rede específica.*" Entendemos que a limitação de acesso a console para uma rede específica ou lista de IPs está relacionado ao fornecimento de uma solução on premises, e que esse tipo de limitação está relacionado a possibilidade de o acesso a console de gerenciamento ser realizado apenas por um determinado endereço IP ou segmento de rede definido pelo TJGO. Soluções ofertada em modelo 100% nuvem, tem por objetivo facilitar o gerenciamento dos dispositivos controlados, ou seja, a possibilidade de o acesso ser realizado através de qualquer lugar através de qualquer endereço IP. Esta exigência está conflitando com as especificações técnicas descritas no Termo de Referência o que consequentemente irá impedir de administradores da solução aplicar correções ou até mesmo analisar um incidente na ferramenta se houver uma restrição de acesso. Devemos entender que a solução não deverá possuir restrição de acesso a console de gerenciamento, uma vez que este acesso é criptografado e somente administradores com credenciais específicas podem acessar a console de gerenciamento. Está correto o entendimento ?

Resposta: Não está correto o entendimento. A restrição de acesso a console de uma rede específica ou a uma lista de endereços IPs não está diretamente ligada à implementação de soluções locais (on premises). Essa restrição de acesso a console de gerenciamento, apresenta maior importância quando se trata de uma solução de segurança totalmente baseada em nuvem. Isso ocorre porque, em uma solução 100% em nuvem, qualquer dispositivo em qualquer parte do mundo pode acessar a console se estiver em posse das credenciais corretas,

Av. Assis Chateaubriand, n° 195, Setor OesteGoiânia, Goiás – CEP 74.130-011 – Telefone (62) 3216-4143/4146 – www.tjgo.jus.br

como nome de usuário, senha e autenticação de segundo fator. A ausência de controle nesse aspecto representa um risco significativo. Isso acontece porque a solução tem a responsabilidade não apenas de proteger os dispositivos, mas também de enfrentar ameaças cibernéticas por meio de ferramentas com acesso privilegiado ao ambiente do TJGO. Um exemplo disso é o requisito 1.22 do Item 1, no Anexo I do Termo de Referência, que requer a execução de comandos críticos no ambiente, tais como "1.22.1 Matar a execução de um processo" e "1.22.3 Reiniciar ou desligar o dispositivo". A má utilização e/ou a exploração dessas ferramentas por um atacante externo poderia levar a incidentes de grande escala. Nesse sentido, a restrição de acesso ao console apenas a partir de uma lista predefinida de endereços IPs específicos ajuda consideravelmente o TJGO mitigar esse risco de forma eficaz.

3) Referente ao plano de instalação da solução ofertada o TJGO possui um quantitativo mínimo no qual a CONTRATADA deverá realizar a instalação?

Resposta: Esclarecemos que, essa informação consta registrada na Seção 9 do Termo de Referência – PLANO DE CONTRATAÇÃO/AQUISIÇÃO (ESTIMATIVA DE CONSUMO):

> *"A expectativa do TJGO é assistir todo o seu parque computacional (aproximadamente 15 mil dispositivos) com a solução tecnológica a ser contratada. O quantitativo pode ser superior ao apresentado, sobretudo em virtude da alteração recente da Organização Judiciária do Estado de Goiás, conforme Lei nº 21.924 de 12 de maio de 2023. Por esse motivo e outros, a presente licitação tem a finalidade de Registro de Preços.*
> *Dessa forma, a estimativa e/ou previsão de consumo ainda será ajustada à data de realização da licitação, bem como à capacidade operacional de configurar o ambiente tecnológico, a fim de evitar desperdícios e possíveis prejuízos à Administração Pública".*

4) Entendemos que é incumbência do fabricante da solução ofertada manter um registro abrangente de todas as modificações efetuadas pelo administrador ao longo de todo o período de validade do contrato, que corresponde a um período de 12 meses. Dessa forma, estabelecemos que tais registros devem ser integralmente preservados ao longo desse período. Está correto o entendimento?

Resposta: Não está correto o entendimento. Será suficiente ao TJGO o atendimento em relação ao requisito 8.1 do Item 1, do Anexo I do Termo de Referência:

> *"8.1.A solução deve fornecer um dashboard que exiba as detecções, o número de novas detecções e as detecções por tipos de ameaças, por pelo menos, os últimos 30 dias."*

5) Ao abordarmos a questão da análise forense em ambientes de elevada complexidade, é essencial considerar a viabilidade de conduzir uma investigação forense de natureza mais minuciosa, visando a identificação da origem primordial do incidente. Nesse contexto, é de suma importância que a solução em questão seja capaz de armazenar integralmente as informações relevantes por um prazo não inferior a 365 dias. Tal abordagem se fundamenta na

necessidade de disponibilizar um histórico detalhado e de longa duração que possibilite a reconstituição e análise aprofundada das circunstâncias que levaram a um incidente em específico. Está correto o entendimento?

Resposta: Não está correto o entendimento. Será suficiente ao TJGO o atendimento em relação ao requisito 8.1 do Item 1, do Anexo I do Termo de Referência:

> *"8.1.A solução deve fornecer um dashboard que exiba as detecções, o número de novas detecções e as detecções por tipos de ameaças, por pelo menos, os últimos 30 dias."*

6) Entendemos que o objeto de contratação do TJGO refere-se à solução de proteção de dispositivos com e inteligência artificial e a capacidade de realizar análise de comportamento, artifícios esses utilizados para uma melhor análise e resposta a um incidente. A adoção da inteligência artificial (IA) pode oferecer uma série de benefícios e vantagens significativas em ambientes de segurança cibernética. Fabricantes que possuem suas soluções baseadas em inteligência artificial são capazes de analisar padrões de comportamento complexos e identificar atividades suspeitas em tempo real. Isso permite uma detecção mais precisa e precoce de ameaças, incluindo ameaças desconhecidas que não podem ser capturadas por soluções que realizam emulação de ameaças em ambientes tradicionais. Entendemos que também será aceito a utilização de IA para monitorar o comportamento dos programas e processos em tempo real, permitindo identificar atividades anômalas ou maliciosas assim que ocorrerem, ao invés de esperar pela execução completa do arquivo dentro de soluções que realizam emulação. Emulações causam lentidões e atrasos que podem impactar na produtividade dos colaboradores do TJGO, visto que quando a solução de proteção de dispositivo não identificar através dos seus motores se o arquivo é malicioso ela irá encaminhar o arquivo para uma emulação em um ambiente secundário para possuir um veredito fazendo uma análise que pode ser burlada caso o atacante utilize mecanismos já conhecidos por cibercriminosos que mascaram o ataque quando o malware identifica que está sendo executado em um ambiente emulado. Entendemos que o intuito deste processo é trazer mecanismos de proteção mais atuais, dinâmicos e ágeis através de predição e análise comportamental.
Diante do exposto entendemos que se a solução ofertada possuir inteligência artificial, análise de comportamento e machine learning capaz de identificar ações maliciosas que garantam a proteção contra arquivos/códigos maliciosos, obtendo um nível de proteção equivalente ou até mesmo superior estas também serão aceitas para o atendimento do item 7 especificado no Termo de Referência, lembrando que esta proteção pode ser comprovada via documentação, laboratório e teste de bancada em ambiente de homologação ou ambiente real para validação de sua efetividade superior. Está correto o entendimento?

Resposta: Não está correto o entendimento. O requisito 7 do Item 1, no Anexo I do Termo de Referência que prevê "Capacidades de emulação de execução de código (Sandbox)", descreve a capacidade da emulação de execução de código de forma integrada à console de gerência 100% em nuvem. Dessa maneira, não haverá lentidões e atrasos que impactem a tecnológica ofertada. Nesse contexto, a solução considerada nas especificações do edital e Termo de Referência não irá depender do veredito somente do Sandbox para proteger o

Av. Assis Chateaubriand, n° 195, Setor OesteGoiânia, Goiás – CEP 74.130-011 – Telefone (62) 3216-4143/4146 – www.tjgo.jus.br

ambiente do TJGO, uma vez que o Termo de Referência exige claramente as funcionalidades de inteligência artificial, análise de comportamento e machine learning, trazendo mecanismos de proteção atuais, dinâmicos e ágeis.

A equipe técnica do TJGO realizou diversos estudos e análises durante a fase de Estudo Técnico Preliminar (ETP), inclusive, por meio de Provas de Conceito (POC), e concluiu que para garantir uma proteção eficaz contra ameaças cibernéticas no seu ambiente interno, é crucial que a solução tecnológica a ser contratada tenha necessariamente a capacidade de emulação de execução de códigos e arquivos. Essa funcionalidade permitirá ao time técnico do TJGO observar o impacto que a execução de um arquivo e/ou conjunto de arquivos ou código(s) maliciosos causará de dano no ambiente de forma antecipada, e, para isso é necessário a capacidade de emulação utilizando o SandBox.

Assim sendo, todo o impacto será medido antes de serem executados no ambiente de produção, identificando assim possíveis ameaças e consequências antes que elas possam ocasionar danos significativos ao equipamento e/ou rede corporativa do TJGO. O resultado da capacidade de emulação de execução de código (Sandbox) também viabiliza a criação de regras de bloqueio com base nos arquivos enviados, sem a necessidade de sacrificar qualquer endpoint/dispositivo para teste.

Por fim, conforme especificado no Anexo I, do Termo de Referência, resta claro que “Será possibilitado que cada empresa licitante combine dois ou mais produtos/softwares/módulos com o objetivo de compor a solução tecnológica exigida neste Termo de Referência, desde que a console de administração da solução seja ÚNICA e 100% DISPONÍVEL EM NUVEM”. Portanto, soluções que não possuem capacidade de emulação de execução de código (Sandbox) não serão aceitas pelo TJGO, pois conforme exigido, para uma eficaz utilização da solução tecnológica se faz necessário que a CONTRATADA atenda todos os requisitos técnicos solicitados.

Goiânia, 30 de agosto de 2023.

GLAUCO CINTRA PARREIRA
Diretor do Núcleo de Contratos e Aquisições de TI
e Integrante Técnico da Contratação

VALDEMAR RIBEIRO DA SILVA JUNIOR
Diretor da Divisão de Suporte a Serviços de TI
e Gestor da Contratação

ANA PAULA RODRIGUES FERREIRA
Pregoeira

Av. Assis Chateaubriand, n° 195, Setor OesteGoiânia, Goiás – CEP 74.130-011 – Telefone (62) 3216-4143/4146 – www.tjgo.jus.br